published by the Department of Energy and or Department of Defense.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

Subpart D—Guides for Original Classification

§ 1203.400 Specific classifying guidance.

Technological and operational information and material, and in some exceptional cases scientific information falling within any one or more of the following categories, must be classified if its unauthorized disclosure could reasonably be expected to cause some degree of damage to the national security. In cases where it is believed that a contrary course of action would better serve the national interests, the matter should be referred to the Chairperson, NISPC, for a determination. It is not intended that this list be exclusive; original classifiers are responsible for initially classifying any other type of information which, in their judgment, requires protection under §1.4 of ''the Order.''

(a) Military plans, weapons systems, or operations;

(b) Foreign government information;

(c) Intelligence activities (including covert activities), intelligence sources or methods, or cryptology;

(d) Foreign relations or foreign activities of the United States, including confidential sources;

(e) Scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) The development, production, or plans relating to the use of weapons of mass destruction.

[78 FR 5118, Jan. 24, 2013]

§ 1203.401 Effect of open publication.

Public disclosure, regardless of source or form, of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosure requires an immediate reevaluation to determine whether the information has been compromised to the extent that downgrading or declassification is indicated. Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. In these cases, if a release were made or authorized by an official Government source, classification of clearly identified items may no longer be warranted. Questions as to the propriety of continued classification should be referred to the Chairperson, NASA Information Security Program Committee.

§ 1203.402 Classifying material other than documentation.

Items of equipment or other physical objects may be classified only where classified information may be derived by visual observation of internal or external appearance, structure, operation, test, application or use. The overall classification assigned to equipment or objects shall be at least as high as the highest classification of any of the items of information which may be revealed by the equipment or objects, but may be higher if the classifying authority determines that the sum of classified or unclassified information warrants such higher classification. In every instance where classification of an item of equipment or object is determined to be warranted, such determination must be based on a finding that there is at least one aspect of the item or object which requires protection. If mere knowledge of the existence of the equipment or object would compromise or nullify the reason or justification for its classification, the fact of its existence should be classified.

§ 1203.403 [Reserved]

§ 1203.404 Handling of unprocessed data.

It is the usual practice to withhold the release of raw scientific data received from spacecraft until it can be calibrated, correlated and properly interpreted by the experimenter under

the monitorship of the cognizant NASA office. During this process, the data are withheld through administrative measures, and it is not necessary to resort to security classification to prevent premature release. However, if at any time during the processing of raw data it becomes apparent that the results require protection under the criteria set forth in this subpart D, it is the responsibility of the cognizant NASA office to obtain the appropriate security classification.

§ 1203.405 Proprietary information.

Proprietary information made available to NASA is subject to examination for classification purposes under the criteria set forth in this subpart D. Where the information is in the form of a proposal and accepted by NASA for support, it should be categorized in accordance with the criteria of § 1203.400. If NASA does not support the proposal but believes that security classification would be appropriate under the criteria of § 1203.400 if it were under Government jurisdiction, the contractor should be advised of the reasons why safeguarding would be appropriate, unless security considerations preclude release of the explanation to the contractor. NASA should identify the Government department, agency or activity whose national security interests might be involved and the contractor should be instructed to protect the proposal as though classified pending further advisory classification opinion by the Government activity whose interests are involved. If such a Government activity cannot be identified, the contractor should be advised that the proposal is not under NASA jurisdiction for classification purposes, and that the information should be sent, under proper safeguards, to the Director, Information Security Oversight Office for a determination.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.406 Additional classification factors.

In determining the appropriate classification category, the following additional factors should be considered:

(a) *Uniformity within government activities.* The effect classification will have on technological programs of other Government departments and agencies should be considered. Classification of official information must be reasonably uniform within the Government.

(b) *Applicability of classification directives of other Government agencies.* It is necessary to determine whether authoritative classification guidance exists elsewhere for the information under consideration which would make it necessary to assign a higher classification than that indicated by the applicable NASA guidance. The Office of Protective Services will coordinate with the Information Security Oversight Office (ISOO) Committee and the National Declassification Center to determine what classification guides are current.

[44 FR 34913, June 18, 1979, as amended at 78 FR 5118, Jan. 24, 2013]

§ 1203.407 Duration of classification.

(a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the timeframe established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the